## CORREIO ELETRÔNICO

- Sempre proteja com senha sua conta de correio eletrônico, seja ele o GroupWise ou qualquer provedor de Internet.
- Não use seu correio eletrônico para propagar mensagens como correntes, piadas, mensagens com anexos suspeitos. Se receber uma dessas, apague-a imediatamente.
- Costumam aparecer mensagens avisando sobre supostos vírus, promessas de brindes ou de produtos milagrosos, heranças, dívidas no SERASA ou em crediários, avisos da Receita Federal, mensagens de bancos, avisos sobre programas com problemas e outros. Essas mensagens são chamadas de phishing scam. Nunca acredite nessas mensagens. Se elas tiverem alguma instrução para você baixar algum programa ou entrar em algum "site" da Internet, seja pelo motivo que for, não faça nada sem confirmar com a CLRI se elas são verdadeiras.
- Cuidado com mensagens contendo anexos, mesmo se forem de pessoas conhecidas. Se você não solicitou a mensagem e não esperava o anexo, apague-a imediatamente.
- Envie cópia de suas mensagens somente para as pessoas necessárias. Verifique sua lista de destinatários antes de mandar.
- E-mail é um canal aberto de comunicação, não o utilize para enviar informação sigilosa, pessoal ou profissional.
- O e-mail da Justiça Federal da 3ª Região deve ser utilizado para fins profissionais.
- Forneça-o apenas para pessoas e empresas que tenham relação com o seu trabalho, e somente para aquelas estritamente necessárias, inclusive pela própria Internet.
- Mensagens oferecendo produtos para venda sem que você as tenha pedido são chamadas de spam. Se o produto não lhe interessa, simplesmente apague a mensagem. Se quiser reclamar, entre em contato com a CLRI.
- Reclamações sobre abusos (spam, mensagens com anexos suspeitos, mensagens oferecendo vantagens suspeitas) podem ser encaminhadas para CLRI@trf3.jus.br ou security@trf3.jus.br.

Guia para

# Segurança da Informação

## na Justiça Federal da 3ª Região

JUSTIÇA FEDERAL **TRF3**

## SEGURANÇA COM NOTEBOOKS

- Quando viajar, mantenha seu notebook perto de você, como bagagem de mão.
- Se viajar de carro não o deixe exposto sobre um banco. Tranque-o no porta-malas.
- Peça para a SETI orientações sobre como manter seu micro sempre atualizado com as últimas correções de segurança e com o antivírus em dia.
- Não o deixe a noite inteira dentro do carro, retire-o quando sair.
- Use um cabo de segurança, que pode ser adquirido pela Justiça Federal da 3ª Região, para amarrar seu notebook à mesa quando estiver num congresso, seminário ou outro evento.
- Proteja suas informações utilizando senha no notebook.
- Se o seu notebook possui capacidade de comunicação com rede sem fio (wireless) nunca o utilize para acessar informação bancária, sigilosa ou pessoal em pontos de acesso públicos como aeroportos, hotéis e restaurantes.
- Nunca deixe seu notebook abandonado em algum lugar, ainda que ele esteja dentro da maleta, mesmo por "um minutinho".
- Nunca o deixe à vista sobre sua mesa de trabalho ou outro móvel no escritório. Tranque-o em algum armário com chave.
- Não use seu cartão de visita como etiqueta de bagagem para identificar a maleta do seu notebook.
- Somente utilize software adquirido oficialmente pela Justiça Federal da 3ª Região.
- Se precisar de um produto peça sua compra.

## SEGURANÇA COM MICROS

- Se sair da sua mesa, desconecte-se (efetue logoff) da rede ou bloqueie a sua estação.
- Acompanhe as orientações da SETI sobre como manter seu micro sempre atualizado com as últimas correções de segurança e com o antivírus em dia.
- Não use protetores de tela baixados da Internet. Use os do sistema.
- A Justiça Federal da 3ª Região não autoriza nem recomenda o uso de mídias removíveis para o transporte de informações confidenciais, cuja divulgação indevida possa trazer qualquer espécie de impacto ou de prejuízo para a Instituição. Caso seja necessário o acesso remoto a elas, pode-se solicitar autorização para o uso da Rede Privada Virtual (Virtual Private Network – VPN), nos termos da Resolução PRES nº 52, de 21 de setembro de 2016.
- Não utilize nenhuma forma de conexão à Internet que não seja aquelas oferecidas pela rede interna ou pelo Wi-Fi corporativo.

## ENGENHARIA SOCIAL

- Engenharia social é utilizada por pessoas maliciosas para conseguir acesso ao seu computador ou a um sistema de uma empresa. O atacante procura aproveitar-se da boa-fé de outras pessoas.
- Nunca forneça qualquer informação pessoal ou de trabalho, principalmente senhas e outras sensíveis, a qualquer pessoa por telefone, mesmo que ela se diga técnica de informática, atendente de banco ou funcionária de empresa.
- Procure destruir papéis que contenham rascunhos de documentos, principalmente se contiverem informações sigilosas. Use um fragmentador. Não os reaproveite.
- Mantenha sua mesa limpa e tranque em lugar seguro documentos de trabalho.
- Se alguém pretendendo ser funcionário de qualquer área da SETI aparecer pedindo "para ver seu micro", tenha a certeza de ter chamado essa pessoa, de que ela diz ser quem é, e o que essa pessoa tem permissão para fazer.

## VÍRUS, WORMS E TROJANS

- Vírus são programas projetados para afetar seu computador.
- Worms são programas que se instalam no seu micro tentando achar falhas em outros micros da rede para aproveitar e se espalhar.
- Trojans são programas que, mesmo parecendo inocentes, carregam algum dos outros programas acima.
- Todos eles podem causar muitos danos, como perda de informação, roubo de senhas de bancos, roubo de informação pessoal sigilosa e outros.
- Não abra arquivos anexados em e-mails sem ter a certeza de que você sabe quem os mandou e sem ter a certeza de que você os pediu.

## SENHAS

- Número máximo de caracteres na senha: 512
- A senha deve ter caracteres de pelo menos 3 das 5 categorias a seguir:
  1. Caracteres maiúsculos de idiomas europeus (caracteres de A a Z, com marcas diacríticas, gregos e cirílicos).
  2. Caracteres minúsculos de idiomas europeus (caracteres de a a z, duplo s, com marcas diacríticas, gregos e cirílicos).
  3. Dígitos de base 10 (0 a 9).
  4. Caracteres não alfanuméricos: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
  5. Caractere Unicode categorizado como um caractere alfabético, mas não em maiúscula ou minúscula, que incluem caracteres Unicode de idiomas asiáticos.
- Você pode usar números em sua senha
- Você pode usar caracteres especiais na senha.
- A senha diferencia maiúsculas e minúsculas.
- Deve ter no mínimo 8 caracteres.
- Deve ter no mínimo 3 tipos dos seguintes caracteres:
  1. Maiúscula (A-Z)
  2. Minúscula (a-z)
  3. Número (0-9)
  4. Símbolo (!, #, $, etc.)
  5. Outros caracteres do idioma não listados acima
- A nova senha não pode ter sido usada anteriormente.

## PROGRAMAS MALICIOSOS (MALWARE)

- São programas criados para finalidades maliciosas, como capturar informações, monitorar sua atividade no computador, capturar senhas e outras informações.
- Para evitar malware, nunca clique em janelas que aparecem no meio da sua página (popups); escolha sempre "Não" ou "No" quando aparecerem perguntas inesperadas; não aceite qualquer tipo de "download".
- Cuidado com software pretendendo ser antivírus ou Antispyware. O único antivírus aprovado para uso na Justiça Federal da 3ª Região é o Symantec Endpoint Protection – SEP – que vem instalado em qualquer estação de trabalho da 3ª Região.
- Se você acredita que o seu micro ou notebook está infectado com algum tipo de artefato malicioso abra um chamado no Callcenter para que ele seja investigado.
- Cuidado com sites que pretendem ser de bancos, de órgãos públicos ou de empresas. Antes de fazer qualquer coisa ou digitar qualquer informação em um site, entre em contato com o banco, empresa ou órgão público e peça instruções para ter certeza de que está no lugar certo.

Este guia é uma publicação da Comissão Local de Resposta a Incidentes – CLRI – com a parceria da Secretaria de Tecnologia da Informação – SETI.

As dicas que apresentamos também podem ser utilizadas, naquilo que couber, para seu micro pessoal e para seu acesso à Internet de casa.

## CONTATO

Comissão Local de Resposta a Incidentes - CLRI
security@trf3.jus.br
Ramal 2030